

CHAPTER 1

INTRODUCTION

0100. REFERENCES AND GUIDANCE. Appendix I lists references (a) through (ae) which are cited in this manual.

0101. DEFINITIONS. For the purpose of this manual, definitions in appendix II apply. The language in this manual separates mandatory standards, measures, or actions from recommended measures or actions.

a. Directive words (e.g., shall, will, must, etc.) indicate that the standard or measure is mandatory.

b. The use of "should" means that the measure or action is required unless the commanding officer has justifiable reason for not implementing the measure or not taking the action. These reasons will be documented during the review and assessment process outlined in this chapter.

0102. PURPOSE. To establish policy and standards for physical security and loss prevention at Navy shore activities. Specifically, this manual:

a. Establishes minimum standards.

b. Provides guidance for evaluating, planning, and implementing each command's Physical Security Program.

c. Relates security measures to assets requiring protection.

d. Provides a basis for determining cost effective security measures/upgrades.

e. Assists those responsible for security in their efforts to carry out their assigned tasks.

0103. OBJECTIVES

a. The objectives of this instruction are to do the following:

(1) Establish general policy for the security of personnel, installations, and certain assets.

(2) Provide realistic guidance, general procedures, and the necessary flexibility for commanders to protect personnel, installations, assets from typical threats.

(3) Reduce the loss, theft, or diversion of, and damage to, Navy assets, thereby ensuring that warfighting capability is maintained.

b. During contingency operations, operations other than war, transition to war, etc., installation and activity commanding officers must provide for adequate protection of forces, personnel and property.

c. This instruction neither voids nor diminishes the authority or responsibility of commands to apply more stringent security standards appropriate for the asset, circumstances, and threat.

0104. SCOPE

a. This manual covers responsibilities for physical security and loss prevention. It classifies various security hazards, details management actions which must be employed to provide an acceptable physical security posture, and selectively sets minimum physical security requirements.

b. This manual applies to all Navy shore installations and activities.

c. This manual places specific emphasis on identification, analyses, and reduction of losses of government property. Physical security is essential to loss prevention.

d. This manual covers matters not covered by other, more specialized security programs.

(1) Protection of classified material, sensitive compartmented information, automated data processing systems, nuclear weapons, conventional arms, ammunition, and explosives, and nuclear reactors and special nuclear material are specifically addressed in references (a) through (f). Those instructions augment the basic guidance provided by this instruction.

(2) Antiterrorism and force protection are addressed in references (g) through (j). Security of Navy and other DoD personnel at U.S. Missions abroad is addressed in reference (k).

(3) Carrying of firearms and use of force, and weapons proficiency training are addressed in references (l) and (m).

e. The Physical Security Program addresses the protection of personnel and property (as such it is inseparably intertwined with antiterrorism and force protection programs). Such protection is accomplished by identifying the property requiring protection, determining jurisdiction and boundaries, assessing the threat, and committing resources to that end.

0105. PHYSICAL SECURITY PROGRAM

a. The physical security program is defined as that part of security concerned with active and passive measures designed

to prevent unauthorized access to personnel, equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft. Physical security is a primary command responsibility.

b. Physical security programs provide the means to counter threats during peacetime transition to war, and in wartime. Physical security threats include the following:

- (1) Foreign intelligence services.
- (2) Paramilitary forces.
- (3) Terrorists and saboteurs.
- (4) Criminals.
- (5) Protest groups.
- (6) Disaffected persons.

0106. SECURITY RESPONSIBILITIES. Specific responsibilities are set forth in the following paragraphs.

0107. CHIEF OF NAVAL OPERATIONS (CNO)

a. The CNO is responsible for formulation and dissemination of Navy physical security policies.

b. The Special Assistant for Naval Investigative Matters and Security (CNO (N09N)) exercises this authority on behalf of the CNO for the Navy. CNO (N09N):

(1) Oversees implementation of Navy physical security and acts as program manager for CNO antiterrorism initiatives.

(2) Performs management, operation, and support functions for all research and engineering of shipboard and waterside security systems; anticompromise emergency destruct systems; explosive detection systems; and locking devices, security containers, and related delay systems. In order to effect appropriate coordination and reduce duplication of efforts, commanders should forward their research, development, test, and evaluation requirements for physical security equipment to CNO (N09N3). Requirements may be forwarded using Mission Need Statements or Operational Requirements documents.

c. Director, Antiterrorism and Force Protection (N34) under the Deputy Chief of Naval Operations (Plans, Policy and Operations (N3/N5) coordinates force protection matters as it relates to naval operations.

0108. Fleet Commanders in Chief (FLTCINCs)/ECHELON 2 COMMANDERS/OTHER ECHELONS OF COMMAND. FLTCINCs, Echelon 2

commanders, and other echelons of command will implement this instruction within their headquarters and subordinate activities, and oversee its implementation. This implementation will include where feasible and appropriate, consolidation and use of physical security resources on a regional basis.

a. The oversight function includes the following:

(1) Develop necessary procedures to meet specific needs, e.g., "campus security", Joint Reserve Bases, etc., for all bases and activities in their area of responsibility. These should be developed on a regional basis where appropriate and feasible.

(2) Coordinate and maintain liaison with the other Echelon 2 commands or Services having installations/activities in the same region(s) as its own, or which share other common interests and concerns.

(3) Develop specific physical security threat assessments, on a regional basis where appropriate and feasible, and keep them up to date.

(4) Oversee training and use of security forces, including consolidation and integration of security forces on a regional basis where appropriate and feasible.

(5) Ensure that all military construction projects are reviewed at the conceptual stage and throughout the process so that appropriate physical security, antiterrorist or force protective design features are incorporated into the design.

(6) Ensure that leases for their Navy activities resident within commercial facilities include provisions for positive physical security (including force protection measures) of Navy-occupied areas.

b. FLTCINCs and other Echelon 2 commands will formalize security procedures for joint response to terrorist incidents and other contingencies.

c. Commands involved with acquisition of major systems will establish internal procedures to ensure inclusion of appropriate security planning for these major systems, as discussed in chapter 2.

0109. THE COMMANDING OFFICER. The commanding officer of an activity is responsible for physical security of that activity and for establishing and maintaining a loss prevention program. The commanding officer will provide sufficient resources to implement, manage and execute an effective physical security and loss prevention program. Commanding officers of tenant activities who require armed security personnel to protect internal assets will coordinate these requirements with the host

installation (or region) commander. In addition to these same responsibilities, the commanding officer of an installation (or region) is also responsible for installation perimeter and area security, including coordination thereof with tenant activities.

0110. THE SECURITY OFFICER. The duties and responsibilities of Navy activity security officers are set out in appendix III.

a. The commanding officer of each Navy activity will appoint in writing a security officer. The security officer may act as security officer, force protection officer, and security manager concurrently. The basic function of the security officer is to assist the commanding officer by:

(1) Determining the adequacy of the command Physical Security and Antiterrorism Program.

(2) Identifying to the commanding officer those areas in which improved physical security and antiterrorism measures are required.

(3) Managing the program on behalf of the commanding officer.

(4) Specific duties expected of the position are outlined in appendix III.

b. The inherent importance of the duties dictates that the security officer must possess mature judgment, and should possess whenever possible:

(1) Appropriate grade/rank.

(2) Security experience appropriate for the mission and operating environment of the activity. Considerations include:

(a) Complexity of the physical security and loss prevention program and resources.

(b) Size of the command or activity.

(c) Size of the security organization.

(3) Occasionally, the security officer function may be a collateral duty, depending upon the size of the activity.

(4) The commanding officer is expected to provide the security officer with sufficient training, resources, staff assistance, and authority to manage and carry out an effective Physical Security and Loss Prevention Program.

(5) Consideration should be given to establishment of an assistant security officer position when the size of the security department exceeds about 100 persons.

0111. ORGANIZATIONAL RELATIONSHIPS. In the performance of assigned duties the security officer acts on behalf of the commanding officer. The security officer collaborates with officers or managers of other specialized security programs within the command concerning physical security needs, threats, requirements, and implementation. The security officer may also serve as the security manager, or manager of other specialized security programs.

0112. THE SECURITY PROBLEM. The security problem is influenced by:

- a. The mission of the activity (e.g., combatant-oriented or training).
- b. The size of the activity.
- c. Who has jurisdiction (e.g., Joint Reserve Bases).
- d. The nature of the property.
- e. The geographic location (e.g., "heartland" or coastal).
- f. The topography of the area.
- g. The economic and political atmosphere (e.g., forward deployed or "campus").
- h. Potential and presumed existing threats.
- i. The degree of support provided by other organizations.

0113. THE SECURITY MANAGEMENT PHILOSOPHY

a. When planning for security, activities must prioritize assets and ensure that each is protected according to its value, vulnerability, and the role it plays in meeting the command's mission. Activity level planners must take basic program standards and requirements and build local procedures that will afford the appropriate degree of protection.

b. Management of security includes risk analysis, which provides the command with a method to rank the mission essential assets against the various threats. This process begins at the activity level, and encompasses the entire region. This analysis serves to:

- (1) Identify assets in a priority order that are most critical for mission accomplishment.

(2) Analyze threats to those assets.

(3) Provide a baseline for managing and prioritizing resources to counter those threats.

0114. COMMAND PHYSICAL SECURITY REVIEW AND ASSESSMENT

a. The commanding officer of a Navy activity is expected to establish a continuing program of systematic physical security review and assessment.

b. During the physical security review and assessment process, the CNO shall be viewed as the "customer" who is being provided the physical security service by the activity.

(1) This manual constitutes the "customer's" standards.

(2) The end objective of the review and assessment processes discussed in this and following paragraphs is to provide physical security, including antiterrorism and force protection, in a manner that meets the pertaining standards at a cost that the "customer" can afford.

(3) Therefore, every activity must review its local processes, in conjunction with host installations, and other activities in the region, to come up with ways of providing physical security that meets the customer's standards in an efficient manner which the customer can afford.

(4) The following are some of the questions that facilitate a review and assessment process:

(a) What are the natures of the threats, and what are the likelihoods that threat events could occur?

(b) What is the activity's mission and what assets are critical to its accomplishment, and require what protection at what cost?

(c) How easily can assets be repaired or replaced?

(d) How does the activity physically protect its assets, and what are the alternatives?

(e) How does the activity link its manpower and financial planning with its security planning?

c. Imaginative thinking may well prove the greatest asset during the review and assessment process. In addition to identifying deficiencies, possible alternatives should be developed as solutions for consideration by the commanding officer.

d. This review and assessment process should include actively seeking local advice and assistance from within the activity regarding the following:

(1) Identifying and prioritizing the mission essential assets and developing vulnerability analyses and the activity threat assessment.

(2) Conducting self assessments of facility for antiterrorism readiness.

(3) Determining requirements for and evaluating security afforded to areas of the activity.

(4) Entry and visitor control procedures and establishment of restricted areas.

(5) Review of draft physical security plans or recommended changes prior to approval by the commanding officer.

(6) Review of command reports of significant missing, lost, stolen, and recovered government property, including loss trends analysis and breaches of security.

(7) Recommendations for improvements to physical security.

(8) Development of security education requirements and materials.

e. Appropriate local participants in such a continuing program of physical security review and assessment include representatives of the following functional areas:

(1) Security officer

(2) Comptroller

(3) Security manager, and officers or managers of other specialized security programs

(4) Public Works Officer or facilities manager

(5) Supply officer

(6) Legal officer or general counsel

(7) All major activity functional area managers whose missions and operations are influenced and impacted by security requirements

0115. INSTALLATION PHYSICAL SECURITY REVIEW AND ASSESSMENT

a. The commanding officer of a Navy installation is expected to establish a continuing program of systematic physical security and loss prevention review and assessment, with goals and purposes similar to that of the individual activity review and assessment programs (see preceding paragraph). But, here specific goals also include:

(1) Vulnerability analysis and assessment of the overall installation.

(2) Preparation of Terrorism Threat Assessment Plan.

(3) Identification of common as well as unique physical security interests and needs of the tenant activities which the host installation must be aware.

(4) Preparation of Physical Security/Force Protection Plan.

(5) Host/tenant coordination and agreements concerning efficient, not alike employment of mutually supportive physical security resources and procedures.

(6) Preparation of Terrorism Incident Response Plan

b. While a command's own individual review and assessment program looks to needs within its organization, the host installation program review and assessment program looks to the needs among the host and tenant organizations, and meeting those needs in an efficient manner. Appropriate participation includes representatives of each tenant activity located on the installation or outlying tenant activities for which physical security and law enforcement are the responsibility of the host command.

0116. REGIONAL PHYSICAL SECURITY REVIEW AND ASSESSMENT

a. The commanding officers of Navy installations within a geographic region are expected to establish a continuing program of systematic physical security review and assessment, with goals and purposes (e.g., terrorism threat assessment planning, force protection planning, and terrorism incident response planning) similar to that of the individual activity and host installation/tenant activity review and assessment programs discussed in the two preceding paragraphs.

b. Yet, specific goals here include identification of employment of specific physical security measures and related antiterrorism and force protection measures that efficiently meet all the security interests and needs of individual activities and installation (host/tenants), in a manner that avoids waste of resources.

c. Therefore, activities and installations must be accurately and completely up-to-date on what their security and force protection interests and needs are. Moreover, they must also have identified all the feasible options for meeting these security and force protection needs, and not become fixated on just one solution. This is a prerequisite for the required flexibility by each participating activity that is necessary for successful security implementation on a regional basis. Regionalization requires that each participating activity have the knowledge to be able to evaluate whether a given course of action could work for them, or to state what adjustments would make the course of action acceptable.

0117. PHYSICAL SECURITY SURVEYS

a. A physical security survey is not an inspection. Instead, it is an in-house formal assessment of an activity's physical security program; including loss prevention, antiterrorism, and force protection. It includes a complete study and analysis of each activity's property and operation, as well as the physical security measures in effect.

b. The intent of these surveys is to update the commanding officer on what needs protecting, what security measures are in effect, and what needs improvement. The survey is also intended to provide the commanding officer with a basis for determining priorities.

c. The results of physical security surveys are key to the activity/installation/regional physical security and loss prevention review and assessment programs described in previous paragraphs. Accordingly, the surveys need to be kept updated so that these review and assessment processes are based on current, complete, and accurate data.

0118. VULNERABILITY ASSESSMENTS

a. Echelon 2 commanders shall ensure physical security vulnerability assessments of facilities, installations, and operating areas within their purview are conducted by either a CNO (N34) or Joint Staff/Defense Threat Reduction Agency team every 3 years. Physical security vulnerability assessments will normally occur at the installation commander level (300 personnel or more) and above. These assessments should consider the range of identified and projected terrorism threats against a specific location or installation personnel, facilities, and other assets. The assessment should identify vulnerabilities and solutions for enhanced protection of DoD personnel and resources. The assessment will address the broad range of physical threats to the security of personnel and assets and shall be conducted at least once every three years.

b. For installations with fewer than 300 personnel, Echelon 2 commands will conduct vulnerability assessments using

CNO (N34) vulnerability assessment checklist every 3 years. Echelon 2 commands may request CNO (N09N) augmentation for guidance within their assessment teams, if needed.

0119. THREAT ASSESSMENTS

a. Liaison with Law Enforcement Agencies. All Naval Criminal Investigative Service (NAVCRIMINSERV) components maintain close and effective liaison with local, State, and Federal law enforcement and intelligence agencies and disseminate, by the most effective means, known threat information affecting the security of a particular military installation. If a command detects or perceives threat information, the servicing NAVCRIMINSERV component should be promptly notified. Follow-up action generally consists of the NAVCRIMINSERV component attempting to obtain amplifying details/intelligence regarding the perceived threat.

b. Evaluation. Based on available information, the command must determine the active short, medium, and long-term threat. The NAVCRIMINSERV can supply these threat evaluations on request. Threat information must be analyzed together with the existing physical security posture to determine if vulnerabilities exist. The possibility of attempts by terrorist groups, criminals, activists, or foreign intelligence operatives to penetrate the security of military installations continues to be a matter of serious concern. Accordingly, NAVCRIMINSERV will provide, upon request, a comprehensive annual area threat assessment through the servicing NAVCRIMINSERV office. Requests should be in writing at least 45 days in advance. The request should specify what threats are of particular concern (terrorism, foreign intelligence, activist and/or criminal), desired method of transmission of the finished report and any unique dissemination requirements.

0120. NEW CONSTRUCTION. All new construction shall comply with the requirements of this manual. Plans for new construction shall be reviewed by the security officer or designated representative during the design process and various review phases to ensure that physical security, loss prevention, antiterrorism, and force protection measures are adequately incorporated. Issues which cannot be resolved at the local level because of lack of necessary funding or other reasons outside the control of the local command (e.g., appropriate and adequate clear zones) will be resolved by the parent Echelon 2 command.

0121. FACILITY MODIFICATIONS. All facility modifications to existing buildings, facilities, sites, etc., shall comply with the requirements of this manual. Proposals for these modifications shall be reviewed by the security officer or designated representative during the design process and review stages to see that physical security, loss prevention, antiterrorism, and force protection measures are adequately incorporated. Issues which cannot be resolved at the local level

because of lack of necessary funding or other reasons outside the control of the local command (e.g., appropriate and adequate clear zones) will be resolved by the parent Echelon 2 command.

0122. NAVY MILITARY CONSTRUCTION PROJECTS. Navy military construction (MILCON) projects must be submitted via the chain of command through CNO (N09N3) to Commander, Naval Facilities Engineering Command. CNO (N09N3) review of physical security construction projects will include ensuring requirements in this manual are addressed (and protective design measures have been considered), and that equipment reliability and maintenance has been considered. Security and force protection can be enhanced by appropriate facility and environmental design. Examples include improved use of lighting and standoff distances.

0123. SECURITY OF LEASED FACILITIES. Terrorist activity worldwide against U. S. military and business concerns poses a clear and persistent danger to Navy interests. Many Navy activities are located within "leased space" facilities and are confronted with unique situations in addressing physical security issues.

a. Commanders shall use the guidance and policies contained in chapters 3 and 5, as applicable, in determining security and/or protective measures deemed essential for their particular spaces, areas and/or buildings. Commands should address physical security in all lease agreements.

b. Liaison with appropriate authorities, e.g., General Services Administration, building administrators, lessors, etc., is essential to delineate specific security responsibilities among the concerned parties regarding measures that are necessary for the protection of lives and property and which are tailored to the individual characteristics of the leased space.

(1) Physical security standards that cannot be met, either temporarily or permanently, must be identified and waiver or exception requests submitted, as appropriate, per paragraph 0124. Compensatory security measures implemented and/or planned must be identified in all such requests.

0124. ACTIVITY UPGRADE REQUIREMENTS/WAIVERS/EXCEPTIONS. All activities will review their existing security posture and determine modifications necessary to conform to this instruction. Basic principles, objectives, and processes must be achieved, and waivers or exceptions to them are not appropriate.

a. A 10 percent deviation from physical security requirements is authorized without need of waiver or exception. New construction, upgrade or modification to existing facilities must conform with standards contained in this manual. A plan of action and milestones will be developed to correct deficiencies.

b. Deficiencies which are not correctable within 12 months will be covered by an approved waiver or exception pending completion of the required upgrade effort. Compensatory security measures are required.

c. Effective with the publication of this manual:

(1) The only provisions authorized for waivers and exceptions to this manual are those outlined here. Any requests for waivers or exceptions to this manual will be submitted per appendix IV.

(2) All existing waivers and exceptions to earlier editions of this manual are cancelled because of extensive revisions here.

d. Blanket Waiver and Exceptions. Blanket waivers and exceptions are not authorized.

e. Waiver and Exception Cancellation. Waivers and long term exceptions are self-cancelling on the expiration dates stated in the approval letters, unless extensions are approved by CNO (N09N3). Cancellations do not require CNO approval.